Network Working Group
Internet-Draft
Updates: RFC8472 (if approved)
Intended status: Standards Track
Expires: April 25, 2019

N. Harper
Google Inc.

October 22, 2018

Token Binding for Transport Layer Security (TLS) Version 1.3 Connections
draft-ietf-tokbind-tls13-02

Abstract

Negotiation of the Token Binding protocol is only defined for Transport Layer Security (TLS) versions 1.2 and earlier. Token Binding users may wish to use it with TLS 1.3; this document defines a backwards compatible way to negotiate Token Binding on TLS 1.3 connections.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 25, 2019.

Copyright Notice

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

1. Introduction

Negotiating Token Binding using a TLS [RFC8446] extension as described in [RFC8472] is fairly straightforward, but is restricted to TLS 1.2 and earlier. Only one minor change is needed to use this extension to negotiate Token Binding on connections using TLS 1.3 and later. Instead of the server putting the "token_binding" extension in the ServerHello like in TLS 1.2, in TLS 1.3 the server puts it in EncryptedExtensions instead.

This document also non-normatively provides a clarification for the definition of the TokenBinding.signature field from [RFC8471], since TLS 1.3 defines an alternate (but API-compatible) exporter mechanism to the one in [RFC5705] used in [RFC8471].

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Token Binding TLS Extension

In TLS 1.3, the "token_binding" TLS extension may be present only in ClientHello and EncryptedExtensions handshake messages. The format of the "token_binding" TLS extension remains the same as defined in [RFC8472].

A client puts the "token_binding" TLS extension in its ClientHello to indicate its support for the Token Binding protocol. The client should follow the same rules for when to send this extension and the contents of its data as in section 2 of [RFC8472]. Since the "token_binding" extension remains unchanged from TLS 1.2 to TLS 1.3 in the ClientHello, a client sending the "token_binding" extension in a TLS 1.3 ClientHello is backwards compatible with a server that only supports TLS 1.2.

A server puts the "token_binding" TLS extension in the EncryptedExtensions message following its ServerHello to indicate support for the Token Binding protocol and to select protocol version and key parameters. The server includes the extension following the same rules as section 3 of [RFC8472], with the following changes:

- The "token_binding" TLS extension is in EncryptedExtensions instead of ServerHello.

- The server MUST NOT include both the "token_binding" extension and the "early_data" extension on the same connection.

3. Interaction with 0-RTT Data

[RFC8446] requires that extensions define their interaction with 0-RTT. The "token_binding" extension MUST NOT be used with 0-RTT unless otherwise specified in another draft. A client MAY include both "early_data" and "token_binding" extensions in its ClientHello - this indicates that the client is willing to resume a connection and send early data (without Token Binding), or negotiate Token Binding on the connection and have early data rejected.

4. Clarification of TokenBinding.signature

This non-normative section provides a clarification on the definition of the TokenBinding.signature field when used on a TLS 1.3 connection.

The Token Binding protocol [RFC8471] defines the TokenBinding.signature field in terms of an exported keying material (EKM) value as defined in [RFC5705]. TLS 1.3 [RFC8446] provides an equivalent interface in section 7.5. For clarity, using the terminology from [RFC8446], the EKM used in section 3.3 of [RFC8471] in TLS 1.3 is the exporter value (section 7.5 of [RFC8446]) computed with the following parameters:

- Secret: exporter_master_secret.

- label: The ASCII string "EXPORTER-Token-Binding" with no terminating NUL.

- context_value: No context value is supplied.

- key_length: 32 bytes.

These are the same input values as specified in section 3.3 of [RFC8471].

5. Security Considerations

The consideration regarding downgrade attacks in [RFC8472] still apply here: The parameters negotiated in the "token_binding" extension are protected by the TLS handshake. An active network

attacker cannot modify or remove the "token_binding" extension without also breaking the TLS connection.

This extension cannot be used with 0-RTT data, so the concerns in [RFC8446] about replay do not apply here.

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[RFC8472] Popov, A., Ed., Nystroem, M., and D. Balfanz, "Transport Layer Security (TLS) Extension for Token Binding Protocol Negotiation", RFC 8472, DOI 10.17487/RFC8472, October 2018, <https://www.rfc-editor.org/info/rfc8472>.

6.2. Informative References

[RFC5705] Rescorla, E., "Keying Material Exporters for Transport Layer Security (TLS)", RFC 5705, DOI 10.17487/RFC5705, March 2010, <https://www.rfc-editor.org/info/rfc5705>.

[RFC8471] Popov, A., Ed., Nystroem, M., Balfanz, D., and J. Hodges, "The Token Binding Protocol Version 1.0", RFC 8471, DOI 10.17487/RFC8471, October 2018, <https://www.rfc-editor.org/info/rfc8471>.

Author's Address

Nick Harper
Google Inc.

Email: nharper@google.com